UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA
EASTERN DIVISION

In re DMS Health Technologies, Inc., Data Breach Litigation	Case No. 3:23-cv-204

DMS HEATH TECHNOLOGIES, INC.'S MOTION TO DISMISS AND MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' AMENDED CONSOLIDATED COMPLAINT

Defendant, DMS Health Technologies, Inc. ("DMS"), through its respective attorneys of record, submits this Motion to Dismiss and Memorandum in support of its Motion to Dismiss Plaintiffs Stacy Kolkind's ("Kolkind") and Constance Boyd's ("Boyd") (collectively "Plaintiffs") Amended Consolidated Class Action Complaint ("Amended Consolidated Complaint") pursuant to Fed. R. Civ. Pro. 12(b)(6) and Fed. R. Civ. Pro. 12(b)(1).

I. INTRODUCTION

Plaintiffs filed separate class action lawsuits after they received notice from Defendant, DMS Health Technologies, Inc. ("DMS"), that it discovered a potential data security event on April 23, 2023, which *may* have involved certain of their Private Information. (Dkt. 36). Just like the original pleadings, there is again no allegation (and there will be no evidence) that any information about either Plaintiff or any putative Class Member is in the hands of the criminals or has otherwise been exposed to third-parties as a result of the reported event. Rather, Plaintiffs allege in the Amended Consolidated Complaint that the unauthorized actor "had the ability to access certain information" and that the criminals had "the intent of engaging in the misuse of Private Information." (*Id*. at ¶¶ 5-6).

Defendants moved to dismiss the twelve-count Original Consolidated Complaint on various grounds. Rather than responding to that Motion to Dismiss, Plaintiffs sought and received leave to file an Amended Consolidated Complaint. The only substantive difference between the two pleadings is that Plaintiffs did not attempt to replead four counts that were clearly subject to dismissal. That said, Plaintiffs did not add any new materially allegations of consequence and dismissal of all eight counts of the Amended Consolidated Complaint is warranted. Instead, Plaintiffs' Amended Consolidated Complaint again asserts a classic "kitchen sink" pleading approach that contains eight counts. All eight counts warrant dismissal under Fed. R. Civ. P. 12(b)(1) and 12(b)(6) due to Plaintiffs' allegations failing to establish standing for any claim or sufficiently state any claim. These counts consist of one statutory claim under North Dakota Central Code § 51-22-02 in addition to seven different common law tort claims, contractual claims, and theories of equitable relief.

In short, Plaintiffs have not alleged a case or controversy under Article III, and their claims do not establish the requisite elements under any relevant law or statute. The North Dakota statutory claim must fail because it requires an active disclosure or affirmative release on the part of a Defendant which is not satisfied when the allegation is that a third-party criminal accessed or stole the information in an alleged data breach. The negligence claim fails to allege a duty. Plaintiffs' three contract claims – breach of implied contract, implied covenant of good faith and fair dealing and third-party beneficiary of a contract – all fail as there is no express contract and some of these causes of action either do not exist in the absence of an express contract or are not recognized at all in the relevant states. The invasion of privacy claim is not clearly recognized in North Dakota and the allegations do not support a claim under other states' laws. The unjust enrichment claim is improper as DMS received no additional benefit for allegedly possessing

Plaintiffs' Private Information. The Declaratory Relief claim fails as Plaintiffs seek a declaration based on a hypothetical set of facts. Therefore, all counts of the Second Amended Complaint should be dismissed with prejudice pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

II. SUMMARY OF PLAINTIFFS' ALLEGATIONS

On September 14, 2024, Plaintiffs filed this Amended Consolidated Complaint on behalf of themselves and purportedly on behalf of a nationwide putative class, a Wisconsin Subclass, and a Minnesota Subclass consisting of all individuals within the United States "whose PHI was exposed to unauthorized third-parties as a result of the alleged data breach discovered by [DMS] on or around April 23, 2023." (Dkt. 36, ¶ 27). Plaintiff Kolkind, an alleged Texas citizen, purports to bring this matter on behalf of a Wisconsin subclass "whose Private Information was exposed to unauthorized third-parties as a result of the event discovered by Defendant on or around April 23, 2023." (*Id*. at ¶ 28). Plaintiff Boyd additionally purports to bring this matter on behalf of a Minnesota subclass "whose Private Information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on or around April 23, 2023." (*Id*. at ¶ 29). Plaintiffs' central allegations of wrongdoing against DMS are that it failed to take steps to adequately safeguard their and Class Members' Private Information and failed to provide timely and accurate notice to them and other Class Members that their Private Information was compromised due to a data breach. (*Id*. at ¶ 44-51).

Plaintiffs allege that they, like Class Members, were required to provide certain Private Information to DMS or DMS's clients in order to receive healthcare services. (*Id*. at ¶ 48). They contend that DMS is a North Dakota corporation with its principal place of business in West Fargo, North Dakota. (*Id*. at ¶ 26). They allege that "upon information and belief," unauthorized third-party cyber criminals gained access to Plaintiffs' and Class Members' Private Information "hosted"

with DMS and that these cyber criminals acted with intent to misuse their and Class Members' Private Information. (*Id.* at ¶ 6). They allege that the "undoubtedly nefarious third party" intends to "profit off this disclosure by defrauding Plaintiffs and Class Members in the future." (*Id.* at ¶ 9). Plaintiffs assert that they and Class Members had a reasonable expectation that DMS would implement safeguards to protect their Private Information. (*Id*. at ¶ 48).

Boyd, a citizen and resident of Minnesota residing in Hinckley, Minnesota, was a patient of Essentia Health Sandstone, which is a client of DMS. (*Id*. at ¶¶ 22-23). She alleges that in order to obtain medical services from DMS, Boyd was required to provide certain "highly sensitive personal and health information." (*Id.* at ¶ 108). She received notice of the Data Breach via a letter dated October 17, 2023. (*Id*. at ¶ 109). Boyd's allegations surrounding her claimed damages are presented *theoretically* as she alleges that: 1) she was injured by the "material risk to future harm"; 2) that this risk is "imminent and substantial"; 3) that there is a "high risk of identity theft or fraud"; and 4) fraud is likely, "given Defendant's clientele, that some of the Class's information … has likely already been misused." (*Id*. at ¶ 114). Further, Boyd alleges that she has been injured in the form of "lost time dealing with the consequences of the Data Breach," the "diminution in value of her Private Information," "increased anxiety" due to the alleged disclosure and "imminent and impending injury" including the "increased risk" of identity theft and fraud. (*Id.* at ¶¶ 113-117). Importantly, Boyd does not allege that she has suffered any out-of-pocket expenses or that the types of injury she fears have actually occurred. (*See, Id.*, generally).

Kolkind, a resident and citizen of Texas residing in Mission, Texas, was a patient of Mayo Clinic in Wisconsin, a client of DMS. (*Id*. at ¶ 15-16). She alleges that she provided her Private Information to Mayo Clinic between March of 2012 and June of 2021. (*Id*. at ¶ 88). Kolkind received notice that her Private Information was potentially exposed via a letter dated September

25, 2023. (*Id*. at. ¶¶ 95-96). She alleges that a hacker gained access to her email account on or around April 22, 2023. (*Id*. at ¶ 92). Kolkind also contends that "she noticed several unauthorized transactions on her Tremendous prepaid card, totaling at least $190." (*Id.*). Kolkind alleges that on or around April 23, 2023, her "Southwest Airlines voucher (valued at $200), was redeemed for the full amount without her knowledge or permission." (*Id*. at ¶ 93).

Kolkind asserts the following damages occurred as a result of the alleged data breach: 1) a "concrete and substantial risk of future harm"; 2) "time and energy spent monitoring her accounts"; 3) "invasion of privacy"; 4) "loss of benefit of the bargain"; 5) "lost time spent on activities remedying harms resulting from the Data Breach"; 6) "lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach"; 7) "diminution of value of her Private Information"; 8) "the continued and increased risk of fraud and identity theft"; 9) "fear, anxiety, and stress" as a result of the Data Breach; and 10) time and money spent monitoring her accounts, including her family's purchase of a $24.99/month credit monitoring service. (*Id*. at ¶¶ 90, 100-105).

Based upon the foregoing, Plaintiffs assert the following causes of action: (1) Negligence; (2) Breach of Implied Contract; (3) Breach of the Implied Covenant of Good Faith and Fair Dealing; (4) Unjust Enrichment; (5) Breach of Contract: Third Party Beneficiary; (6) Invasion of Privacy; (7) Declaratory Relief; and (8) Violation of N.D. Cent. Code § 51-22-02. Plaintiffs purport to bring all of these causes on their own behalf and on behalf of the putative classes set forth above.

III. MOTION TO DISMISS STANDARD

DMS moves to dismiss the Amended Consolidated Complaint under Rule 12(b)(6) for Plaintiffs' "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), "a complaint must contain sufficient factual

matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While "[t]he plausibility standard is not akin to a 'probability requirement,'" it does require "more than a sheer possibility that a defendant has acted unlawfully" and a complaint that only pleads facts "that are 'merely consistent with' a defendant's liability" will "stop [] short of the line between possibility and probability." *Id*. at 678 (internal citations omitted). Legal conclusions "must be supported by factual allegations" and a Court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Id*. at 678-79 (quoting *Bell Atl.,* 550 U.S. at 555); Finally, "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." And in "[d]etermining whether a complaint states a plausible claim for relief," the Court is required to "draw on its judicial experience and common sense." *Id*. at 679.

In ruling on a motion to dismiss under Rule 12(b)(6) this Court "may rely on materials 'necessarily embraced by the pleadings,' including exhibits attached to the complaint and matters of public record." *Buckley v. Hennepin Cnty*., 9 F.4th 757, 760 (8th Cir. 2021) (citation omitted); see also *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 715 (8th Cir. 2017). "[W]hen a written instrument contradicts allegations in the complaint . . . the exhibit trumps the allegations." *Elkharwily v. Mayo Holding Co*., 955 F. Supp. 2d 988, 996 (D. Minn. 2013) (citation omitted). Here, DMS relies only on Plaintiffs' pleading and nothing outside the pleading (other than common sense) to attack Plaintiffs' Amended Consolidated Complaint. Accordingly, all citations to the docket herein are to Plaintiff's Complaint, which is Docket No. 36.

DMS also moves to dismiss Plaintiffs' claims for failing to establish standing under Fed. R. Civ. Pro. 12(b)(1). In order for a federal court to have subject-matter jurisdiction, a Plaintiff must establish the three Article III standing requirements: (1) the Plaintiff must have suffered an

injury in fact, (2) there must be a fairly traceable causal connection between the injury and the conduct complained of, and (3) it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *McGowen, Hurst, Clark & Smith, P.C. v. Commerce Bank*, 11 F.4th 702, 709 (8th Cir. 2021) (citing *Sanzone v. Mercy Health*, 954 F.3d 1031, 1046 (8th Cir. 2020)). An injury in fact requires "an invasion of legally-protected interest which is (a) concrete and particularized and (b) actual and imminent, not conjectural or hypothetical." *Sierra Club v. Robertson,* 28 F.3d 753, 758 (8th Cir. 1994). "Traceability requires proof of causation, a showing that the injury resulted from the actions of the defendant and not from the independent action of some third party not before the court"—that is, the injury is "fairly traceable to the challenged action of the defendant." *McGowen*, 11 F.4th at 709 (quoting *Miller v. Thurston*, 967 F.3d 727, 734, 735 (8th Cir. 2020)).

In diversity cases, such as this one, standing to sue under the relevant state law must exist in addition to Article III standing. *Wolfe v. Gilmour Mfg. Co.*, 143 F.3d 1122, 1126 (8th Cir. 1998). Standing under state common law or statutory claims turns to the specific common law or statutory requirements of each type of claim advanced by Plaintiff. As discussed in detail below, the relevant states include North Dakota, Minnesota, and Texas

Plaintiffs seeking a declaratory judgment under 28 U.S.C. § 2201 must meet these same Article III standing requirements. *McGowen*, 11 F.4th at 709. There must be a concrete dispute between parties having adverse legal interests, and the declaratory judgment Plaintiff must seek "specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." *Maytag Corp. v. Int'l Union, United Auto., Aero. & Agric. Implement Workers of Am.*, 687 F.3d 1076, 1081 (8th Cir. 2012) (quoting *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 241, 57 S. Ct. 461, 81 L. Ed. 617 (1937)).

In the declaratory judgment context, the difference between an actual case or controversy and a hypothetical state of facts is a question of degree. *Id*. "Basically, the question in each case is whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *Id*. (quoting *Md. Cas. Co. v. Pac. Coal & Oil Co.*, 312 U.S. 270, 273 (1941)).

IV. CONFLICTS OF LAW

This Court has very recently held that at the motion to dismiss stage in an alleged data breach class action, the Court should look to the laws of the forum jurisdiction and the states of citizenship of the Plaintiffs and analyze the common-law claims under the laws of all of those states and not perform a full conflicts of law analysis until the discovery stage. *Quaife,* 2024 U.S. Dist. LEXIS 92051, at *5. Here, DMS is alleged to be a North Dakota corporation with its principal place of business in North Dakota, Boyd a citizen of Minnesota and Kolkind a citizen of Texas. Oddly, Kolkind seeks, in the alternative of a nationwide class, to be the representative Plaintiff for a Wisconsin subclass consisting of all individuals "within Wisconsin" even though she is neither a Wisconsin resident nor citizen. "Named plaintiffs lack standing to assert claims under the laws of the states in which they do not reside or in which they suffered no injury." *Insulate SB, Inc. v. Advanced Finishing Sys.*, 2014 U.S. Dist. LEXIS 31188, at *34 (D. Minn. Mar. 11, 2014). Because Kolkind does not reside in Wisconsin, nor does she allege to incur any injuries within the state of Wisconsin, since she provided her data to DMS's client in 2021, she does not have standing to assert a Wisconsin subclass. Accordingly, for purposes of this motion, the common law claims will be analyzed under the laws of North Dakota, Texas and Minnesota pursuant to the *Quaife* Court's very recent instruction.

V. ARGUMENT

All eight of Plaintiffs' claims set forth in their Amended Consolidated Complaint must be dismissed with prejudice pursuant to Fed. R. Civ. P. 12(b)(1) and Fed. R. Civ. P. 12(b)(6). As described in detail below, Plaintiffs' allegations neither establish requisite standing, nor do they sufficiently state any claim.

1. Plaintiffs' Claims Must Be Dismissed Under 12(b)(1) Because They Do Not Allege Any Injury In-Fact Fairly Traceable to Any Action by Defendant.

This matter cannot be heard by this Court unless Plaintiffs have asserted an actual case or controversy. As explained, this requires an injury in fact that is concrete and particularized, not speculative or hypothetical. Additionally, the cause of the injury must be traceable to the actions of Defendant, not a third-party. Neither Plaintiff Kolkind nor Plaintiff Boyd have established both of these factors.

A. Plaintiffs' Common Law and Statutory Claims Must Be Dismissed Under 12(b)(1) Because They Do Not Allege an Injury In Fact Fairly Traceable to Any Action by Defendant.

Plaintiffs' Amended Consolidated Complaint cannot support a finding of an injury in fact which is traceable to Defendant, rather than a third party. The Complaint starts out by asserting Plaintiffs' and Class Members' sensitive personal data including names, dates of birth, dates of service, physician names, and exam types were not reasonably secured, leading to damages. (Dkt. 36, ¶ 1). However, they later state that Plaintiffs are in the dark regarding what particular data was potentially accessed by the unauthorized actor. (*Id*. at ¶ 49). Similarly, at the beginning of their Complaint, Plaintiffs allege that that an "undoubtedly nefarious third party" sought to profit off the "disclosure" to them by defrauding Plaintiffs and Class Members in the future. (*Id.* at ¶ 9). Then, they proceed to allege that Plaintiffs and Class Members are "left to speculate" as to "who has used it, and for what *potentially* nefarious purposes." (*Id.* at ¶ 50). These inconsistent

allegations indicate that Plaintiffs cannot allege any injury in fact without it being entirely rooted in speculation, as they have not suffered any injuries exposing that their information was indeed accessed.

Plaintiffs lack of a concrete injury in fact is further evidenced by their specific alleged injuries. When detailing Plaintiff Kolkind's injuries, the Complaint alleges that a hacker, around the time of DMS's data security event, gained access to her email, resulting in unauthorized charges to a prepaid credit card of hers totaling $190, and her $200 Southwest Airlines voucher being redeemed. (*Id.* at ¶¶ 90 – 94). It is unclear how this could be achieved through the misuse of any of the alleged Personal Information Plaintiffs alleged to be accessed. There are no allegations regarding any further similar activity that Plaintiff Kolkind has suffered since April 2023. Plaintiff Boyd, based on the allegations, has not experienced anything similar to Plaintiff Kolkind, I.E.: she has not experienced unauthorized charges of any sort. The other claimed injuries of both Plaintiffs include: time spent mitigating the impact of the event, monitoring accounts, diminution of value of Private Information, continued and increased risk of identity fraud, fear/anxiety/stress related to potential harm.

Plaintiffs cannot fulfill the Article III standing requirements based on these injuries. The only concrete harm suffered by either Plaintiff is Plaintiff Kolkind's alleged unauthorized charges, but Plaintiffs failed to allege any causal connection between this incident and the DMS's data security event. The fact that this happened around the same time of the breach is not sufficient correlation to show causation, particularly because it is entirely unclear how this alleged hacking could be a result of the data that Plaintiffs claim was accessed. This is the only evidence Plaintiffs set forth showing any potential misuse, and this misuse has in no way been linked to DMS. Because no actual misuse has occurred, an alleged diminution in value of their private information is also

not sufficient to support standing. *See Dusterhoft v. Onetouchpoint Corp.*, 2024 U.S. Dist. LEXIS 170993, at *19-20 (E.D. Wis. Sep. 23, 2024) (plaintiffs could not establish standing based on conclusory allegations of a diminution in the value of their private information without evidence of misuse).

Plaintiffs' claims that they have lost time monitoring and mitigating cannot constitute an injury in fact unless they have adequately alleged a risk of future harm. *Alleruzzo v. SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017). In order to establish standing based on a risk of future harm, the complaint must allege a certainly impending or substantial risk of future harm. *Id.* at 769. In *SuperValu*, it was held that risk of future misuse is not substantial if the information accessed by an authorized party is not, collectively, the type of information that could plausibly lead to identity theft or the opening of fraudulent accounts. *Id.* at 770-71. Although Plaintiffs, later into their Complaint, allege they are unsure exactly what information was accessed, they initiate the Complaint with stating that the information that was compromised was their names, dates of birth, dates of service, physician names, and exam types. Taking those allegations as true, it is unquestionable that an account cannot be made, nor could identity fraud be carried out with only these categories of "identifiers." Thus, Plaintiffs' allegations do not establish a substantial risk of harm, so their mitigating and monitoring do not support standing, nor have Plaintiffs adequately alleged they are *actually* at an increased risk of identity fraud.

Likewise, their allegations do not establish a certainly impending future harm. Plaintiffs attempt to argue that misuse can occur "up to a year or more" following a security event. (Dkt. 36, at ¶ 83). At this point, it has been "a year or more" since the data was allegedly accessed, and Plaintiffs have not alleged to experience any misuse distinctly tied to the data DMS possessed. Lastly, they claim that this event has caused them fear, anxiety, and stress related to potential

misuse, but Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013). Therefore, none of Plaintiffs alleged injuries support standing.

Even if Plaintiffs could establish injury in fact, they certainly have not alleged that any purported injury is fairly traceable to DMS rather than a third party. Any injury would be solely traceable to the bad actor who illegitimately accessed DMS's stored data. DMS did not actively allow or participate in the potential dissemination of Plaintiffs' and Class Members' information. Further, Plaintiffs cannot allege any certain type of data security measures that would have certainly prevented this data breach. Every business is at risk of sophisticated cyber criminals hacking into their system, regardless of the type of security measures or how much they cost. To say that a different type of security system would have prevented this event is entirely speculatory and cannot support standing. Accordingly, the common law and statutory claims should be dismissed with prejudice pursuant to Fed. R. Civ. Pro. 12(b)(1).

B. The Declaratory Judgment Count Must Be Dismissed for Lack of Standing Under 12(b)(1) Because Plaintiffs Allege Only Abstract Future Injury.

Based upon Plaintiffs' allegations and the alleged risk of future harm, they lack standing to assert the claim for Declaratory Judgment under Fed. R. Civ. Pro. 12(b)(1). *See Hall v. Centerspace, LP,* 2023 Dist. LEXIS 83438, at *7 – 13 (D. Minn. 2023). Plaintiffs' claim for Declaratory Judgement, in specific, is predicated solely on the hypothetical instance that DMS suffers a future data security event and the further hypotheticals that their information is impacted and that DMS did nothing to enhance security practices. (Dkt. 36, ¶¶ 218 – 222). The Court in *Hall* addressed this very theory and concluded that in a data breach case like this, in order to establish standing and show that the hypothetical future harm is "sufficiently imminent" there must be

specific facts pled to "indicate that a second data breach is certainly impending, or even that there is a substantial risk that one will occur." *Hall,* 2023 Dist. LEXIS at *10.

DMS acknowledges that this Court in *Quaife* held that there were sufficient allegations to establish standing since the plaintiff had alleged a "risk of harm and injury in fact as to the stolen personal information." *Quaife,* 2024 U.S. Dist. LEXIS at *14. However, here and like as in *Hall,* the Declaratory Judgement action is not based upon information that was allegedly already subject to access. Rather, is relates solely to the alleged possibility of a future data breach. There is simply no allegation that there is somehow another data breach on the horizon. After all, any company in the world could be subject to a data breach. But that speculative possibility is not enough for Article III standing. Accordingly, the Count VII claim for Declaratory Judgement should be dismissed with prejudice pursuant to Fed. R. Civ. Pro. 12(b)(1).

2. Plaintiffs' Claims Must be Dismissed Under 12(b)(6), as They Have Failed to Allege the Requisite Elements to Sufficiently State Any Claim.

All of Plaintiffs' claims have fatal flaws that require dismissal under Fed. R. Civ. Pro. 12(b)(6) for failure to state a claim. The North Dakota Central Code claim is not at all applicable to the case at bar. The contractual claims fail as none are based on an express contract and DMS took no action that would create an implied contractual obligation. The unjust enrichment claim fails as DMS retained no benefit. The negligence claim fails for lack of duty. Thus, these claims must be dismissed with prejudice.

A. Plaintiffs Count VIII Claim for an Alleged Violation of N.D. Cent. Code § 51-22-02 Must Be Dismissed as Such a Claim Cannot be Predicated Upon the Alleged "Inaction" of Failure to Secure One's Computer Network.

A very recent decision from this Court made clear that the "disclosure" prohibition in North Dakota Century Code Sec. 51-22-02 ("the ND Non-Disclosure Act") requires some "some type of

action" and that the alleged "inaction" of the failure to safeguard personal information from a cyberattack is not a "disclosure" for purposes of the statute. *Quaife*, 2024 U.S. Dist. LEXIS at *14-15. The provision of the ND Non-Disclosure Act at issue provides:

> No business entity which charges a fee for data processing services ***may disclose*** in whole or in part the contents of any record . . . .which is prepared or maintained by such business entity to any person, other then the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity. N.D. Cent. Code § 51-22-02. N.C. Cent. Code § 51-22-02 (Emphasis supplied).

In *Quaife,* the class action Plaintiffs alleged a violation of the ND Non-Disclosure Act in a data breach class action where the central allegation of wrongdoing was:

> "Defendant disclosed Plaintiffs' and Class Members' PI to third parties without their consent by failing to take appropriate measures to safeguard and protect that PI amidst a foreseeable risk of a cybersecurity attack resulting in the Data Breach." *Id.* at *12-13.

The court reasoned that although the term "disclosure" does not require willfulness or ill-intent, "it does require some sort of action" on the defendant's part and that the allegation of wrongdoing above is based upon alleged "inaction." *Id.* at *14. Accordingly, the Court dismissed Plaintiffs' ND Non-Disclosure Act for failure to state a claim stating: "There is no accusation that [Defendant] transferred, published, or distributed the personal information to a third party. The allegations are that cyber criminals accessed [Defendant's] computer system and stole the information." *Id.* at *13.

There is simply no basis to distinguish this case from *Quaife*. In fact, the above-quoted allegation of wrongdoing found in the *Quaife* case is the ***verbatim allegation*** found in Plaintiffs' Complaint in the ND Non-Disclosure Act count in this case:

> "Defendant disclosed Plaintiffs and Class Members' Private Information to third parties without their consent by failing to take appropriate measures to safeguard and protect that Private Information amidst a foreseeable risk of a cybersecurity attack, resulting in the Data Breach." (Dkt 36, ¶ 228).

As Plaintiffs' allegations are based upon the exact type of "inaction" which occurred in *Quaife*, they do not amount to disclosure and Plaintiffs' Count Eight claim under the ND Non-Disclosure Act must be dismissed with prejudice for failure to state a claim.

B. Plaintiffs Fail to Allege Any Conduct on the Part of DMS That Gives Rise to a Claim for Breach of Implied Contract.

To state a claim for breach of an implied contract, a plaintiff must plead the existence of a valid implied contract, performance or tendered performance by the plaintiff, breach of the implied contract by the defendant, and damages resulting from the breach." *Electrostim Med. Servs., Inc. v. Health Care Serv. Corp.*, 614 F. App'x 731, 744 (5th Cir. 2015). In all relevant jurisdictions, the elements of breach of contract are the same for express or implied, but the question of whether a contract exists in the implied contract setting is based upon the objective manifestations of the parties through words and actions. *Id.* (Texas Law); *Hall,* 2023 Dist. LEXIS at *14 (Minnesota law); *Lord & Stevens, Inc. v. 3D Printing, Inc.,* 2008 ND 189, 756 N.W.2d 789, 792 (N.D. 2008).

Here, Plaintiffs point to no objective conduct by DMS evidencing a contractual promise to secure their data. In fact, Plaintiff Boyd alleges she had no knowledge that DMS even had her data. (Dkt. 36, ¶ 112). Further, both Plaintiffs allege that they tendered their information to other parties – the Mayo Clinic and Essentia Health Sandston. (*Id*. at ¶¶ 18, 107). At a minimum, Plaintiffs must plead what words, actions or other manifestations DMS made (and not those of the Mayo Client or Essentia Healthcare Sandstone) that would lead Plaintiff to believe they had a contract with DMS that included data security provisions. *See, e.g.*, *Alleruzzo v. SuperValu, Inc.,* 870 F.3d 763, 771 (8th Cir. 2017) (finding plaintiffs did not become parties to an implied contract to protect PII simply by giving defendant their payment information); *Alleruzzo v. SuperValu, Inc.*, 925 F.3d 955, 965-66 (8th Cir. 2019); *Cmty. Bank of Trenton v. Schnuck Mkts.,* No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *5 (S.D. Ill. May 1, 2017) (finding "implicit promise" of data security

insufficient to support implied contract claim), *aff'd*, 887 F.3d 803 (7th Cir. 2018). Accordingly, Plaintiffs have failed to properly plead facts to establish the existence of an implied contract claim and the Count II claim must be dismissed with prejudice.

C. Plaintiffs Cannot State a Claim for Breach of Implied Covenant of Good Faith as the Claim is Either Not Recognized, Very Narrow, or Cannot Exist in the Absence of an Express Contract.

Although there is some minor variance in the laws of North Dakota, Texas and Minnesota as to this claim, it is clear that under all of these states' jurisprudence, dismissal is required because Plaintiff does not even plead the existence of an express contract, but rather a generic implied contract. Initially, North Dakota flatly rejects such a claim, as North Dakota courts and courts applying North Dakota Law have repeatedly held that the cause of action does not exist outside of the insurance contract setting. *See, e.g.,* W*FND, LLC v. Fargo Marc, LLC*, 2007 ND 67, 730 N.W.2d 841, 851 (N.D. 2007); *Pitchblack Oil, LLC v. Hess Bakken Invs. II, LLC*, 949 F.3d 424, 428 (8th Cir. 2020). Specifically, the North Dakota Supreme Court has repeatedly held that such a claim cannot survive even when there is a concrete written contract and that the *only* exception to this general rule is for insurance contracts. *Id., See also, Barnes V. St. Joseph's Hospital,* 1999 ND 204, 601 N.W.2d 587 (N.D. 1999). The North Dakota Supreme Court explained:

> "In North Dakota, the doctrine of an implied covenant of good faith and fair dealing has only been applied to insurance contracts. Moreover, the implied covenant of good faith and fair dealing . . . . does not operate to alter the material terms of a contract. . .. nor does the duty of good faith inject substantive terms into the parties' contract."

WFND, LLC, 730 N.W.2d at 851; *See also, Pitchblack Oil,* 949 F.3d at 428 ("North Dakota does not apply the implied covenant of good faith and fair dealing to any contract other than an insurance agreement").

Texas courts also recognize that the cause of action is extremely limited. *Indep. Fin. Grp., LLC v. Quest Trust Co*., U.S. Dist. LEXIS 236718 (S.D. Tx. 2022). Specifically, "not all contracts

contain an implied covenant of good faith and fair dealing." *Houle v. Casillas*, 594 S.W.3d 524, 544 (Tex. App. 2019) citing *Saucedo v. Horner*, 329 S.W.3d 825, 831-32 (Tex. App.—El Paso 2010, no pet.)). The claim "is a tort action that arises from an underlying contract." *Saucedo*, 329 S.W.3d at 831. Texas differs from other states in that "contracting parties owe a good-faith duty only if they expressly agree to act in good faith, a statute imposes the duty, or the parties have a 'special relationship' like that between an insurer and insured." *Dallas/Fort Worth Int'l Airport Bd. v. Vizant Techs., LLC*, 576 S.W.3d 362, 369 n.13 (Tex. 2019) (citing *Subaru of Am. v. David McDavid Nissan, Inc.*, 84 S.W.3d 212, 225 (Tex. 2002)). Only in cases where there is a special relationship, such as between an insurer and its insured, does Texas law impose an actionable duty of good faith and fair dealing. *Id.* Whether the duty exists is a question of law. *Id.*

Finally, under Minnesota law, although every contract includes an implied covenant of good faith and fair dealing, the doctrine is applied to ensure that one party not "unjustifiably hinder" the other party's performance of a specific contractual obligation. *In re Hennepin Cnty. 1986 Recycling Bond Litigation*, 540 N.W.2d 494, 502 (Minn. 1995); *Churlik Gate City Bank*, 2024 U.S. Dist. LEXIS 20090, at *4 (Dist. Minn. 2024). Accordingly, a party acts in bad faith if it refuses "to fulfill some duty or contractual obligation based on an ulterior motive." *Kivel v. WealthSpring Mortg. Corp.*, 398 F.Supp.2d 1049, 1057 (D. Minn. 2005). Moreover, merely seeking to maximize profits is insufficient to show bad faith. *BP Prods. N. Am., Inc. v Twin Cities Stores*, 534 F. Supp. 2d 959, 967 (D. Minn. 2007).

Here, Plaintiffs do not allege the existence of an express contract, but rather an implied contract based upon alleged actions of DMS. So, Plaintiffs' claim is for breach of an implied covenant of good faith and fair dealing included in an alleged implied contract. Obviously, if the North Dakota Supreme Court does not inject an implied covenant of good faith and fair dealing

into express written or oral contracts it certainly would not inject such an implied covenant into an alleged implied contract with no defined terms. Further, under Texas law there is certainly no preexisting "special relationship" like the insurer-insured that would lead to the legal creation of such a claim in the absence of even an actual express contract. Finally, and relevant to Minnesota law, there is no allegation that DMS has an ulterior motive in itself being the victim of a data security event or that it tried to hinder Plaintiffs from performing a contractual obligation. After all, Plaintiffs claim their only obligation was to tender their Private Information. In short, the claim for Breach of Implied Covenant of Good Faith and Fair Dealing is flawed under all relevant state laws and must be dismissed with prejudice pursuant to Fed. R. Civ. P 12(b)(6).

D. Plaintiffs Have Not Stated a Claim for Unjust Enrichment as They Do Not Allege That DMS Failed to Provide the "Services" They Sought or That DMS Was Paid Extra for "Data Protection."

Unjust enrichment is an equitable doctrine which rests upon contract or quasi-contract theories of recovery and a benefit conferred by one party at the unjust expense of another. As the North Dakota Supreme Court succinctly stated, "the essential element in recovering under the theory of unjust enrichment is the receipt of a benefit by the defendant from the plaintiff which would be inequitable to retain without paying for its value." *McDougal v. AgCountry Farm Credit Servs, PCA,* 937 N.W.2d 546, 553 (N.D. 2020). Minnesota and Texas courts apply the same standards. *See e.g., Hall,* 2023 U.S. Dist. LEXIS at *18 (D. Minn.); and *Heldenfels Bors., Inc. v. City of Corpus Christi,* 832 S.W.2d 39, 41 (Tex. 1992).

In *Quaife,* this Court rejected an unjust enrichment claim in the data breach context under both North Dakota and Minnesota law because there can be no unjust enrichment if there is no direct relationship between the plaintiffs and defendant. *Quaife,* 2024 U.S. Dist. LEXIS at *11-12. This Court held that there could not be a direct relationship between Plaintiffs and Defendant in

Quaife because the Defendant contracted with Plaintiffs' *employer* for accounting services, not Plaintiffs directly, and Plaintiffs did not allege that their employer did not receive the benefit of the bargain. *Id*. at *11. Because there was no benefit conferred to the Defendant by the Plaintiffs, it was held that Plaintiffs had not plausibly alleged unjust enrichment, and the claim was dismissed. *Id*. at *11 – 12.

Additionally, a recent case from the District of Minnesota held the Plaintiffs could not state an unjust enrichment claim in the data breach context because there was no indication that Plaintiffs paid more to "secure data security than those who did not provide PII." *Hall,* 2023 Dist. LEXIS at *21 – 22. Finally, the Eighth Circuit Court's opinion in *Alleruzzo v. SuperValu, Inc.* 925 F.3d 955 (8th Cir. 2019), although it applied Illinois state law to an Unjust Enrichment claim, is instructive. *Id.* at 966. The Plaintiff alleged that the Defendant supermarket paid for groceries with a credit card and that her information was later obtained by the hackers. Plaintiff alleges that had she known of a data breach, she would not have shopped at Defendant's store. *Id.* The Court rejected plaintiff's argument and dismissed the unjust enrichment claim, holding that Plaintiff concedes she received her groceries and did not pay a premium for data security. The court explained:

> Common sense counsels against the viability of [plaintiff's] theory of unjust enrichment. Holmes paid for groceries. The price would have been the same whether he paid with cash or a credit card. He did not pay a premium for a 'side order of data protection'. *Id.*

The exact same logic applies here. Plaintiffs claim to have tendered personal information "to Defendant for the purpose of obtaining health services." (Dkt. 36, ¶ 178). Further, they allege that they "did not receive the benefit of their bargain because they paid for health care products/and or health care services that did not satisfy the purposes for which they bought them." (*Id.* at ¶ 183). Plaintiffs' ambiguousness is purposeful, as, when they provided their Private Information, it was

for the purpose of obtaining health care services, which they did in fact receive, from the unnamed parties whose employees or agents provided the sought after medical treatment. As Plaintiffs state in their complaint, DMS contracts with its clients for imaging services. (Dkt. 36, ¶ 191). Just as in *Quaife*, no direct relationship exists between Plaintiffs and Defendant because DMS is not who they were seeking a benefit from in exchange for providing their information with payment, nor are they who contracted with DMS.

Further, Plaintiffs, at no point, allege that they paid a premium to DMS for the protection of their Private Information. Plaintiffs attempt to claim DMS was benefitted because it "received profits and other benefits by failing to invest in reasonable security measures to protect the Plaintiffs' data, thus saving costs while continuing to benefit financially from Plaintiffs' trust." (Dkt. 36, ¶ 177). This allegation is, on its face, entirely conclusory and speculative, as they have not alleged any facts to even remotely support this. This is Plaintiffs' attempt to negate the fact that they did not pay any additional amounts for the protection of their data. Further, it cannot be assumed true that more expensive data security measures than what DMS was using at the time of the incident would ensure reasonableness or that a breach would be entirely prevented. Cost and level of protection are not directly related, especially in the realm of data security. Regardless, it is undisputed that Plaintiffs did not pay any extra amount to either DMS for the protection of their data, thus, their allegations do not support a claim of unjust enrichment.

Even if Plaintiffs could show a direct relationship, Plaintiffs fail to sufficiently allege that DMS received any benefit or that they did not receive the specific health care services they sought when they provided their Private Information to entities which are not parties to this lawsuit. Accordingly, Count IV for unjust enrichment must be dismissed with prejudice under Rule 12(b)(6).

E. Plaintiffs Cannot State a Claim For Breach of Contract on a Third-Party Beneficiary Theory For a Number of Reasons.

A third party may recover on a contract made between other parties only if the parties intended to secure a benefit to that third party, and only if the contracting parties entered into the contract directly for the third party's benefit. *MCI Telecomms. Corp. v. Texas Util. Elec. Co.*, 995 S.W.2d 647, 651 (Tex. 1999). A third party does not have a right to enforce the contract if she received only an incidental benefit. *Id.* "A court will not create a third-party beneficiary by implication." *Id.* Rather, an agreement must clearly and fully express an intent to confer a direct benefit to the third party. *Id.* Further, "it must appear by express stipulation or by reasonable inference that that the rights and interests of such unnamed parties were contemplated and the provision was made for them." *McShane Construction Co., LLC v. Gotham Ins. Co.,* 867 F. 3d 923, 930 (8th Cir. 2017). Minnesota has adopted the "intended beneficiary approach" wherein there must be an express duty owed to the third-party in the contract or that the beneficiary is the intended beneficiary of the promised performance. *Hickman v. Safeco Ins. Co. of America,* 695 N.W.2d 365, 369 (Minn. 2005). Again, merely being an "incidental beneficiary" of a contract is not enough. *Id.*

Here, Plaintiffs fall woefully short of establishing they have a right to enforce any contract between DMS and some unnamed "clients" of DMS. To wit, Plaintiffs vaguely allege that "[DMS] and [DMS's clients] contracted for imaging services" and that "upon information and belief" these contracts included promises to "provide data retention and security services" and comply with laws and industry standards. (Dkt. 36, ¶¶ 191 – 192). DMS is left to assume that Plaintiffs are alleging the existence of contracts between DMS and the Mayo Clinic (Kolkind) and DMS and Essentia Health Sandstone (Boyd). Even if such contracts exist, Plaintiff speculatively alleges that "[u]pon Plaintiff's information and belief, Defendant's contracts with clients, among other things,

promised to take reasonable measures to safeguard and protect such information for the benefit of Plaintiffs and the Class." (*Id*. at ¶ 194). These claims are entirely speculative assumptions of the Plaintiffs, as they do not have access to these alleged contracts between DMS and their "clients." Further, based on the products and services that DMS provides, it is without that question that the nature of any agreement between DMS and its clients or customers is not at all similar to a will or trust agreement where the ***express intent*** of the contract is to benefit a third-party. Rather, assuming *arguendo*, there are data security provisions in these hypothetical contracts with DMS's clients, Plaintiffs would be, at best, incidental beneficiaries of those provisions, in light of the collection of their data being incidental to receiving these clients' services.

Any contractual obligation to safeguard data would be for the general benefit of the party contracting with DMS, with Plaintiffs being the unintended beneficiaries of the agreement. This is not enough. Accordingly, Count V must be dismissed with prejudice pursuant to Fed. R. Civ. Pro. 12(b)(6).

F. Plaintiffs' Claim for Invasion of Privacy Must Be Dismissed as Plaintiffs Voluntarily Tendered Their Information and They Allege That it Was a Third-Party Criminal That Tried to Steal Their Information – Not DMS.

Although not specifically labeled as such, Plaintiffs' Count VI claim for Invasion of Privacy is based upon an intrusion upon seclusion theory as they allege that the "unauthorized release" of their Private Information was "highly offensive" and that this "intrusion was into a place or thing." (Dkt. 36, ¶¶ 206 – 207). In North Dakota, it is unclear if the tort of invasion of privacy based upon an intrusion upon seclusion even exists. *Hogum v. Valley Memorial Homes,* 574 N.W.2d 812, 818 (N.D. 1998). In Minnesota, intrusion upon seclusion is when someone "intentionally intrudes, physically or otherwise, upon the solitude of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." *Lake v. Walmart*

Stores, Inc. 582 N.W.2d 231, 233 (Minn. 1998); *In re Grp. Health Plan Litig.,* No. 23-cv-267 (JWB/DJF), 2023 U.S. Dist. LEXIS 227218, at *6 (D. Minn. Dec. 21, 2023). In Texas, "Usually an action for intrusion upon one's seclusion is found only when there has been a physical invasion of a person's property or ... eavesdropping on another's conversation with the aid of wiretaps, microphones, or spying." *Graham v. JPMorgan Case Bank, Nat. Ass'n*, 2015 U.S. Dist. LEXIS 93045, (S.D. Tex. July 15, 2015) (quoting *Ross v. Midwest Commc'ns, Inc.*, 870 F.2d 271, 273 (5th Cir. 1989)).

Here, there can be no claim for intrusion upon seclusion because DMS did not "intrude" upon Plaintiffs in anyway. Rather, as Plaintiff clearly alleges, they willfully gave their Private Information to DMS or DMS's client and it was allegedly stolen or criminally accessed by an unknown third-party criminal. So, if anyone "intruded" upon Plaintiffs' seclusion, it was the criminal and not DMS. A federal district court in Wisconsin recently addressed this claim and succinctly addressed the issue. *Linman v. Marten Transp.,* 2023 U.S. Dist. LEXIS 45661 (W.D. Wis. 2023) (applying Wisconsin law). In *Linman,* the Court, applying Wisconsin law in an alleged data breach class action extremely similar to the case at bar, explained how an Invasion of Privacy – Intrusion Upon Seclusion claim cannot exist under Wisconsin law because the Plaintiff admits it voluntarily gave its PII to the Defendant and that it was a third-party and not the Defendant who was alleged to have improperly stolen it. *Id.* at *12. The court explained:

> Linman hasn't stated a claim for intrusion upon seclusion for one simple reason: ***it was the hackers, not Marten, that intruded on Linman's privacy***. Linman provided his personal information to Marten willingly, so it didn't intrude on his privacy by collecting it. The only "intrusion" was the alleged breach by the hackers. (Emphasis supplied).

Id.; *See also, In re Group Health Plan Litigation,* 2023 U.S. Dist. LEXIS (D. Minn 2023) (court found Plaintiff plausibly stated intrusion upon seclusion claim under Minnesota law where it

installed tracking pixel software on its website and collected Plaintiff data without its consent and voluntarily shared it with third-parties for marketing and data analytic purposes).

Here, Plaintiffs do not allege that DMS unlawfully obtained their Private Information. Rather, they allege they voluntarily tendered in the information. Plaintiffs do not allege that DMS voluntarily shared their information with a third-party. Rather, they allege DMS was itself a victim of a cyberattack wherein criminals attempted to steal the information. Given these facts, this Court should follow the logic of *Linman* and dismiss with prejudice Plaintiffs' claim for invasion of privacy.

G. The Negligence Claim Fails as Plaintiffs' Allegations to Establish a Legal Duty are Insufficient and Vague.

DMS acknowledges that this Court recently recognized the possibility that a Defendant may owe a duty "at least at this early stage" of litigation to have sufficient data security measures because a data breach may be foreseeable. *Quaife,* 2024 U.S. Dist. LEXIS 92051 at *8. However, this Court also recognized that such a duty must be established through "sufficient factual allegations" as to both foreseeability, the entrustment of data and a connection with the personal information stolen.

Here, Plaintiffs' allegations of the nature of the relationship between themselves and DMS are contradictory and vary from paragraph to paragraph. For example, the Complaint describes Plaintiff Kolkind as "providing her Private Information to Mayo Clinic… a healthcare provider that relied on Defendant." (Dkt. 36, ¶ 18). Within the same paragraph, it states that if she would have known her data wasn't being adequately protected, "she would not have entrusted Defendant with her Private Information or allowed Defendant to maintain this sensitive Private Information." (*Id*.). The same claims are asserted in terms of Plaintiff Boyd. (*Id*. at ¶ 24). Importantly, it is explicitly stated that Plaintiff Boyd was entirely unaware that Defendant even had possession of

her data. (*Id*. at ¶ 112). Yet, the Complaint states she "entrusted" her Private Information to Defendant. (*Id*. at ¶ 115). In short, Plaintiffs cannot have it both ways.

DMS is not necessarily saying that Plaintiffs may not potentially be able to allege a duty, but they have not in the Amended Consolidated Complaint. DMS understands that Plaintiffs can plead claims in the alternative, but they cannot plead facts in the alternative. In short, Plaintiffs' contradictory and vague allegations call into question the nature and scope of any duty owed by DMS to Plaintiffs and the negligence claim must be dismissed with prejudice.

VI. CONCLUSION

Based upon the arguments and authorities contained herein, Defendant DMS Health Technologies Inc., respectfully requests that this Honorable Court dismiss all counts of Plaintiffs' Amended Consolidated Complaint with prejudice pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

Respectfully submitted:

O'HAGAN MEYER LLC

/s/ James W. Davidson
James W. Davidson, Admitted *Pro Hac Vice*
O'Hagan Meyer LLC
One East Wacker Drive, Suite 3400
Chicago, Illinois 60601
(312) 422.6100 – T
jdavidson@ohaganmeyer.com
Attorney for Defendant, DMS Health Technologies, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on October 9, 2024, all counsel of record who are deemed to have consented to electronic service are being served a true and correct copy of the foregoing document using the Court's CM/ECF system:

Todd Michael Miller
Solberg Stewart Miller
PO Box 1897
Fargo, ND 58107-1897
701-237-3166
tmiller@solberglaw.com

MIGLIACCIO & RATHOD LLP
Nicholas A. Migliaccio, Admitted *Pro Hac Vice*
412 H Street N.E., Suite 302
Washington, D.C. 20002
T: (202) 470-3520
nmigliaccio@classlawdc.com

/s/ James W. Davidson
James W. Davidson, IL ARDC No. 6281542
O'Hagan Meyer LLC
One East Wacker Drive, Suite 3400
Chicago, Illinois 60601
312.422.6100 –T
312.422.6110 – F
jdavidson@ohaganmeyer.com